

BIG SUCCESS OR “BIG BROTHER?”: GREAT BRITAIN’S NATIONAL IDENTIFICATION SCHEME BEFORE THE EUROPEAN COURT OF HUMAN RIGHTS

Jennifer Morris\*

TABLE OF CONTENTS

I. INTRODUCTION ..... 445

    A. *The United Kingdom’s Identity Cards Act* ..... 445

    B. *The Security-Privacy Debate* ..... 446

    C. *The Privacy Landscape in the United Kingdom* ..... 447

    D. *Overview* ..... 449

II. PRIVACY IN THE UNITED KINGDOM ..... 450

    A. *Early Domestic Law* ..... 450

    B. *Changes in the Privacy Landscape—The Data Protection Act and the Human Rights Act* ..... 451

        1. *The Data Protection Act* ..... 451

        2. *The Human Rights Act* ..... 454

    C. *Public Opinion* ..... 455

        1. *Public Support for the Identity Cards Act* ..... 455

        2. *Public Response to Previous National Identification Schemes in the United Kingdom* ..... 456

        3. *Three Objections to the Identity Cards Act* ..... 457

        4. *The Response of Other Governmental Entities* ..... 458

III. THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND ITS PROTECTION OF THE RIGHT TO PRIVACY ..... 459

    A. *The Convention* ..... 459

    B. *Article 8 Interferences (Triggers)* ..... 460

    C. *“In Accordance with the Law”* ..... 461

    D. *Legitimate Aims* ..... 463

    E. *“Necessary in a Democratic Society”* ..... 463

---

\* J.D., University of Georgia School of Law, 2008; B.A., University of Georgia, 2005.

IV. GREAT BRITAIN'S NATIONAL IDENTIFICATION SCHEME: THE IDENTITY CARDS ACT 2006 .....	464
<i>A. Background</i> .....	464
<i>B. The National Identity Register and "Registrable         Facts"</i> .....	465
<i>C. Entry on the Register</i> .....	466
<i>D. Disclosure of Information Contained on the Register</i> .....	466
<i>E. Phasing In</i> .....	466
<i>F. Benefits</i> .....	467
V. ANALYSIS UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS .....	467
<i>A. Article 8 Interference</i> .....	467
<i>B. "In Accordance with the Law"</i> .....	469
<i>C. Legitimate Aims</i> .....	469
<i>D. "Necessary in a Democratic Society"</i> .....	470
VI. CONCLUSION .....	471

## I. INTRODUCTION

The terrorist attacks of September 11, 2001, rekindled public debate about a National Identification Scheme (NIDS) in the United States and in many other countries throughout the world. As with most other national security measures enacted since September 11, the proposal of a NIDS involves striking a balance between security and liberty, therefore generating considerable debate worldwide. Although the debate is by no means new,<sup>1</sup> the issue has resurfaced with vigor in today's age of global terrorism. Feeling the need to improve identity verification systems and to attempt to curb fraudulent procurement of identity documents by terrorists, a number of countries throughout the world have seriously considered the use of a NIDS to improve national security.<sup>2</sup>

*A. The United Kingdom's Identity Cards Act*

The United Kingdom, a country that has been plagued by terrorism long before the rise of Middle Eastern extremist groups, has recently come up with a NIDS of its own.<sup>3</sup> The United Kingdom has been attacked by terrorists associated with the Irish Republican Army for decades,<sup>4</sup> and has been the

---

<sup>1</sup> Approximately one hundred countries around the world currently use national identification cards. See Simon Davies, *Identity Cards: Frequently Asked Questions*, PRIVACY INT'L, Aug. 24, 1996, available at [http://www.privacy.org/pi/activities/idcard/idcard\\_faq.html](http://www.privacy.org/pi/activities/idcard/idcard_faq.html); DAVID BANISAR ET AL., PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND INTERNATIONAL DEVELOPMENTS 27 (2002) ("ID cards are in use in one form or another in virtually all countries of the world. The type of card, its functions, and integrity vary enormously. [A] number of countries have official, compulsory national ID cards that are used for a variety of purposes. . ."). Examples of countries with some form of a national ID card include Belgium, France, Germany, Greece, Malaysia and South Africa. *Id.* Other countries, including the United States, have struggled with the idea of a NIDS for years. See *National ID Cards and REAL ID Act*, ELEC. PRIV. INFO. CTR. (stating that proposals to initiate a NIDS failed in the United States in 1971, 1976 and 1999), available at [http://www.epic.org/privacy/id\\_cards/default.html](http://www.epic.org/privacy/id_cards/default.html) (last visited Mar. 24, 2008).

<sup>2</sup> Since September 11, 2001, China, Malaysia and Finland have adopted some variation of a NIDS. See generally Rina C.Y. Chung, *Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America*, 4 ASIAN-PACIFIC L. & POL'Y J. 518, 562 (2003).

<sup>3</sup> See Identity Cards Act, 2006, c. 15 (Eng.).

<sup>4</sup> For a discussion of the United Kingdom's history with the Irish Republican Army (I.R.A.), see Clive Walker, *Constitutional Governance and Special Powers Against Terrorism: Lessons from the United Kingdom's Prevention of Terrorism Acts*, 35 COLUM. J. TRANSNAT'L L. 1 (1997)

target of a recent Al-Qaeda attack.<sup>5</sup> These situations led to a climate in which security from terrorism is of utmost importance to its citizens. Britain's Identity Cards Act of 2006 has been termed by some as "the most ambitious project of its kind and one of the world's largest [information technology] schemes."<sup>6</sup> In essence, the NIDS will require all British subjects over the age of sixteen to enter personal information into a National Identity Register.<sup>7</sup> In its early stages, only those individuals applying for a passport will be issued an identification card,<sup>8</sup> but the British government plans to make the cards, complete with basic identity information and biometric data, available to all British subjects as early as 2010.<sup>9</sup>

### B. The Security-Privacy Debate

Implementation of a NIDS raises two fundamental issues: security and privacy. The use of digital and biometric technology makes a NIDS, such as the one envisioned by the British Identity Cards Act, a more reliable source of verification.<sup>10</sup> Proponents argue that such systems will make it more difficult for terrorists to obtain fraudulent forms of identification.<sup>11</sup> Furthermore, by allowing government agencies to cross-reference information, a NIDS facilitates watch-lists thereby allowing governments to identify potential threats to national security.<sup>12</sup>

---

("Political violence connected with [The Irish Republican Army] has been a significant and continuous cause of death and destruction within Great Britain since . . . 1973. . . . [R]egularly occurring attacks . . . have caused over 120 deaths in Britain.")

<sup>5</sup> On July 7, 2005, an Al-Qaeda affiliated group set off a series of three bombs in the London subways, killing fifty-two and wounding more than seven hundred. The attacks were described as the worst in Great Britain since World War II. See Alan Cowell, *Subway and Bus Blasts in London Kill at Least 37*, N.Y. TIMES, July 8, 2005, at A1; Jim VandeHei, *Bush Defends Strategy Against Terrorist Attacks; London Bombs Meant to Scare U.S., President Says*, WASH. POST, July 12, 2005, at A3.

<sup>6</sup> *Britain's Ambitious ID Card Plan Comes Under Attack*, REUTERS NEWS, Aug. 4, 2006.

<sup>7</sup> Identity Cards Act, 2006, c. 15, § 1 (Eng.).

<sup>8</sup> Home Office, *How the National Identity Scheme Will Get Started*, <http://www.ips.gov.uk/identity/scheme-what-how.asp> (last visited Mar. 24, 2008).

<sup>9</sup> Home Office, *How to Get Your ID Card and How It Will Be Produced*, <http://www.ips.gov.uk/identity/scheme-what-produced.asp> (last visited Mar. 24, 2008).

<sup>10</sup> Neda Matar, Comment, *Are You Ready for a National ID Card? Perhaps We Don't Have to Choose Between Fear of Terrorism and Need for Privacy*, 17 EMORY INT'L L. REV. 287, 313 (2003).

<sup>11</sup> See *id.*

<sup>12</sup> *Id.* at 313-14.

On the other hand, a NIDS has serious implications for privacy. The ability of the government to combine sensitive personal information into one centralized database raises legitimate concerns about the possibility of intrusive government surveillance of citizens.<sup>13</sup> This objection is reflected in the appreciative public response to novels such as George Orwell's *1984*.<sup>14</sup> In addition to government access to private data, critics fear employers, landlords, credit agencies, direct mailers and other interested parties will access information contained in the national databank, further implicating privacy concerns.<sup>15</sup>

The British Identity Cards Act, shaped by tortured debate on these issues, remains a heated topic of controversy.<sup>16</sup> While advocates claim the scheme is needed to fight against terrorism, organized crime, and illegal immigration, critics fear the scheme will ultimately lead to impermissible privacy intrusion and civil liberties infringements.<sup>17</sup>

### C. *The Privacy Landscape in the United Kingdom*

Privacy rights are recognized around the world,<sup>18</sup> and Great Britain is no exception. Although Great Britain does not have a written constitution, the right to privacy has been protected by various common law doctrines and statutes.<sup>19</sup> In most cases, the right to privacy is protected only incidentally to the protection of some other right or value, and the right to privacy does not

---

<sup>13</sup> *Id.* at 308–09; see also American Civil Liberties Union, National ID Cards: 5 Reasons Why They Should be Rejected, Sept. 8, 2003, <http://www.aclu.org/privacy/gen/14898res20030908.html> [hereinafter National ID Cards].

<sup>14</sup> GEORGE ORWELL, 1984 (1949) (depicting a totalitarian society in which an omnipotent dictator ("Big Brother") monitors people's thoughts and actions; the term "Big Brother" has come to refer to a ruler or government that invades the privacy of its citizens).

<sup>15</sup> National ID Cards, *supra* note 13.

<sup>16</sup> *Britain's Ambitious ID Card Plan Comes Under Attack*, *supra* note 6; Mark Trevelyan, *British ID Scheme Seen as Key Biometrics Test*, REUTERS NEWS, Nov. 23, 2004.

<sup>17</sup> Trevelyan, *supra* note 16.

<sup>18</sup> *Privacy and Human Rights 2003: Overview*, PRIVACY INT'L ("Privacy is recognized around the world in diverse regions and cultures. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international treaties. . . . In many countries, international agreements that recognize privacy rights such as the International Covenant on Civil and Political Rights or the European Convention on Human Rights have been adopted into law."), available at <http://www.privacyinternational.org/survey/phr2003/overview.htm> (last visited Mar. 24, 2008).

<sup>19</sup> See HOME OFFICE, LORD CHANCELLOR'S OFFICE, SCOTTISH OFFICE, REPORT OF THE COMMITTEE ON PRIVACY 25–28 (1972).

appear to be the main consideration of such laws.<sup>20</sup> Nevertheless, these early common law doctrines and statutes have provided the groundwork for the protection of the right to privacy in the United Kingdom.

The greatest protection for privacy in the United Kingdom came in 1998 when Parliament approved two Acts with expansive implications for that right: the Data Protection Act and the Human Rights Act.<sup>21</sup> The Data Protection Act covers records held by both government agencies and private entities and sets limitations on the use of, access to, and maintenance of personal information.<sup>22</sup> The Human Rights Act is by far the greatest protection for privacy the United Kingdom has ever seen. The Act incorporated the European Convention on Human Rights, an international agreement that includes a specific right to privacy,<sup>23</sup> into domestic law, thus effectively establishing for the first time in Great Britain an enforceable right to privacy.<sup>24</sup>

The right to privacy in the United Kingdom is also backed by the force of public opinion. Although public concern over the right to privacy is not as strong in Great Britain as in other countries around the world,<sup>25</sup> there is, on some levels, strong public recognition of the right to privacy. In fact, public opinion regarding the use of national identification cards in the past demonstrates the public's strong desire to protect the interest of privacy. The United Kingdom has faced proposals to establish national identity cards in the past, all failing in the face of public objection.<sup>26</sup>

---

<sup>20</sup> *Id.* at 25.

<sup>21</sup> Data Protection Act, 1998, c. 29 (Eng.); Human Rights Act, 1998, c. 42 (Eng.).

<sup>22</sup> Data Protection Act, 1998, c. 29 (Eng.).

<sup>23</sup> David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 105 (1999).

<sup>24</sup> BANISAR ET AL., *supra* note 1, at 375.

<sup>25</sup> For example, Great Britain has used Closed-Circuit Television Surveillance to monitor its citizens since 1985, and this practice has not been met with much public resistance or challenge. See SURVEILLANCE, CLOSED CIRCUIT TELEVISION AND SOCIAL CONTROL 9 (Clive Norris et al. eds., 1998) ("[A]s the rise of [Closed Circuit Television] Surveillance easily evokes Orwellian concerns of Big Brother, we may ask why there has been so little public resistance or challenge."). In addition, some criminal and public laws have been passed in recent years with significant implications for the right to privacy. See Banisar & Davies, *supra* note 23, at 106.

<sup>26</sup> *National ID Cards and REAL ID Act*, *supra* note 1.

*D. Overview*

Given Great Britain's longstanding history and strong public support of protecting a right to privacy, the legitimacy of the Identity Cards Act is dubious. Great Britain is faced with serious threats to national security, as are many other countries around the world, and its interest in providing for the welfare of its citizens is of utmost importance. Indeed, national security is one of the greatest duties owed to the citizenry of any country, and should not be undertaken lightly. However, as this Note demonstrates, a comprehensive NIDS such as the Identity Cards Act is not the answer. National security, although perhaps the strongest government interest that might justify interference with civil liberties, is by no means a blank check to ignore basic civil rights. Instead, as the jurisprudence of the European Court of Human Rights in interpreting Article 8 of the European Convention on Human Rights indicates, the two interests of security and liberty should be weighed against each other.<sup>27</sup>

Part I of this Note will discuss the privacy picture in the United Kingdom, including the various common law doctrines and statutes with privacy elements, the Data Protection Act, the Human Rights Act that incorporated the European Convention of Human Rights into domestic law, as well as public opinion regarding privacy in general in the United Kingdom. Part II will discuss in further detail the protections provided by the European Convention on Human Rights, which has been incorporated into domestic English law.

Part III will explore the various provisions of the Identity Cards Act and will show the extent to which the Act invades the privacy interest. The Act has been described as "the most ambitious project of its kind and one of the world's largest [information technology] schemes."<sup>28</sup>

Finally, Part IV will analyze the Identity Cards Act under the European Court of Human Rights. Analysis under the European Court of Human Rights essentially has four steps: (1) Is there an interference with the privacy interest?; (2) Is the interference with the privacy interest in accordance with domestic law?; (3) Does the interference with the privacy interest serve one of the legitimate aims listed in Article 8.2?; and, (4) Is the interference with the privacy interest necessary and appropriate to the aim it serves?

---

<sup>27</sup> European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR], available at <http://conventions.coe.int/Treaty/en/Treaties/Word/005.doc>.

<sup>28</sup> *Britain's Ambitious ID Card Plan Comes Under Attack*, *supra* note 6.

In conclusion, this Note will demonstrate the utter failure of the Identity Cards Act to pass European Court of Human Rights muster. Although the topic will continue to be debated in the United Kingdom, as well as in other areas throughout the world, national identification systems—at least the one envisioned by the Identity Cards Act—are dangerous intrusions upon civil liberties in the name of national security. Countries throughout the world will face the challenges of balancing security and liberty in the context of combating terrorism for many years to come. However, no country need sacrifice the cherished civil liberties it has worked for centuries to develop, simply to ensure that it will continue to endure in the face of terrorism and other breaches of national security. The two interests are not mutually exclusive.

## II. PRIVACY IN THE UNITED KINGDOM

### *A. Early Domestic Law*

Although there is no per se legal right to privacy in the United Kingdom, the law does provide privacy protection scattered throughout common law doctrines and statutes.<sup>29</sup> In some of these laws, the protection of privacy is only incidental to the protection of other rights and values.<sup>30</sup> For example, the common law proscription against trespass to land protects the right to privacy, but that protection is only secondary to the property right.<sup>31</sup> Other laws, such as defamation, libel, and slander, protect rights that are very similar to and co-extensive with privacy, such as the control of personal information.<sup>32</sup> The early common law tort of breach of confidence is likely the closest that the United Kingdom ever came to an outright recognition of the right to privacy<sup>33</sup> in controlling the right to use personal information.<sup>34</sup> The laws of contract and copyright also control the use of personal information.<sup>35</sup>

---

<sup>29</sup> HOME OFFICE, *supra* note 19, ¶ 83, at 25 (“There is no legal right to privacy as such in the law of England and Wales. . . . [T]he protection that the law in Great Britain gives is scattered throughout civil and criminal law, both common and statute.”).

<sup>30</sup> *Id.*

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> *Id.* at 25–26 (“The law on breach of confidence offers the most protection of privacy in all existing law.”).

<sup>34</sup> *Id.* at 25.

<sup>35</sup> *Id.*



In addition to these common law and statutory tort offenses, Britain's criminal regulatory scheme includes statutes that afford protection for the right to privacy.<sup>36</sup> The protection is scattered throughout several criminal laws, each aimed at a particular offense.<sup>37</sup> The right to privacy does not appear to have been the central aim or concern in any of these statutes, but the protection is afforded nonetheless, even if only incidentally.<sup>38</sup> Examples of criminal laws that protect privacy interests include proscriptions against sending offensive telephone messages; opening another's mail; sending obscene or indecent matter through the post; harassing tenants; and harassing debtors.<sup>39</sup>

Some of the biggest protections of the privacy interest in early United Kingdom law dealt with the right to acquire and use personal information.<sup>40</sup> As previously mentioned, copyright laws and the laws against breach of confidence were aimed at the acquisition and use of personal information.<sup>41</sup> The Wireless Telegraphy Acts also afforded some protection by criminalizing the use of wireless telegraphy transmitting apparatus without a license; the use of wireless telegraphy transmitting apparatus for the interception of non-public messages; and the import and manufacture of wireless telegraphy transmitting apparatus.<sup>42</sup> In certain instances, criminal laws also prohibit the selling of employee information by employers.<sup>43</sup> The laws also protect against industrial espionage and "bugging" without a wire."<sup>44</sup>

## *B. Changes in the Privacy Landscape—The Data Protection Act and the Human Rights Act*

### *1. The Data Protection Act*

Prior to 1984, legal protection of privacy in the United Kingdom was relatively sparse and much less protective than the privacy laws of other nations throughout the world.<sup>45</sup> However, faced with the growing threat from

---

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> *Id.* at 27.

<sup>40</sup> *See, e.g., id.*

<sup>41</sup> *Id.* at 25.

<sup>42</sup> *Id.* at 27.

<sup>43</sup> *Id.*

<sup>44</sup> *Id.*

<sup>45</sup> *Id.*

increased computer use around the 1970s and the accompanying ease with which groups could rapidly compile information, the United Kingdom recognized the need for more comprehensive privacy protection.<sup>46</sup> Parliament met that need by passing the first Data Protection Act 1984,<sup>47</sup> one of the first laws of its kind.<sup>48</sup> For the first time, individuals and groups who held personal data about individuals were required to register with the Office of the Data Protection Registrar.<sup>49</sup> The purpose of the Data Protection Act was to set limits on the acquisition, use and disbursement of personal information held by both private entities and government agencies.<sup>50</sup> The Data Protection Act is guided by eight principles for the proper processing of personal data.<sup>51</sup> For example, the information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.<sup>52</sup> Furthermore, personal data shall be held only for one or more specified and lawful purposes, and personal data held for any purpose shall not be used or disclosed in any manner incompatible with that purpose.<sup>53</sup> Of particular relevance is the requirement that personal data held for any purpose shall be adequate, relevant, and not excessive to that purpose.<sup>54</sup>

Additionally, the Data Protection Act stipulates that an individual shall be entitled, at reasonable intervals and without undue delay or expense, to certain rights regarding the data. These rights include the right to be informed of any data held concerning the individual subject,<sup>55</sup> a description of any such data

---

<sup>46</sup> PETER CAREY, DATA PROTECTION: A PRACTICAL GUIDE TO UK AND EU LAW 1 (2d ed. 2004) ("The desirability of data protection legislation arose out of the growing use of computers in the 1970s and the threat to personal privacy that rapid manipulation of data potentially posed. In the UK the existing law at that time (which consisted of not much more than a possible action in breach of confidence) was insufficient to deal with concerns about the amount of information relating to individuals that was held by organizations in electronic form.").

<sup>47</sup> Data Protection Act, 1984, c. 35 (repealed 1998) (Eng.). The law was later updated and repassed in 1998. See Data Protection Act, 1998, c. 29 (Eng.).

<sup>48</sup> CAREY, *supra* note 46, at 3.

<sup>49</sup> Data Protection Act, 1998, § 17(1).

<sup>50</sup> *Id.* long title.

<sup>51</sup> *Id.* sched. 1, pt. I.

<sup>52</sup> *Id.* sched. 1, pt. I(1).

<sup>53</sup> *Id.* sched. 1, pt. I(2).

<sup>54</sup> *Id.* sched. 1, pt. I(3).

<sup>55</sup> *Id.* § 7(1)(a).

held by a data user,<sup>56</sup> and, where appropriate, to have such data corrected or erased.<sup>57</sup>

The Data Protection Act was modified extensively in 1998, largely in response to a directive of the European Union requiring all Member States to pass national legislation with regard to the processing of personal data.<sup>58</sup> The principle aims of this European Union directive, known as the Data Protection Directive, were the “protection of an individual’s privacy in relation to the processing of personal data” and the “harmonization of data protection laws of the Member States.”<sup>59</sup> The United Kingdom’s Data Protection Act of 1998, which was in response to the European Union Data Protection Directive, changed the regime of the 1984 Act in significant ways.<sup>60</sup> For example, new conditions were imposed for processing.<sup>61</sup> A new category of information—sensitive personal data—was created, which must not be processed unless certain conditions are met.<sup>62</sup> These sensitive personal data categories include personal data consisting of information as to—

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union,
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offense,  
or
- (h) any proceedings for any offense committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.<sup>63</sup>

---

<sup>56</sup> *Id.* § 7(1)(b)(i).

<sup>57</sup> *Id.* § 14(1).

<sup>58</sup> CAREY, *supra* note 46, at 5.

<sup>59</sup> *Id.* at 6.

<sup>60</sup> *Id.* at 5 (“The new Act . . . took data protection legislation to a new level of complexity in the UK.”).

<sup>61</sup> Data Protection Act, 1998, c. 29, § 17.

<sup>62</sup> *Id.* § 2.

<sup>63</sup> *Id.*

The Act also created significantly more and stronger individual rights, including the right to compensation in cases of unlawful processing.<sup>64</sup> Other rights protected in the Data Protection Act 1998 include the right of access to personal data;<sup>65</sup> the prevention of processing likely to cause damage or distress;<sup>66</sup> the prevention of processing of personal data for direct marketing;<sup>67</sup> the prevention of automated decision-taking;<sup>68</sup> the right to rectification, blocking, or erasure and destruction of inaccurate personal data;<sup>69</sup> and the right to request assessment.<sup>70</sup> However, the right to individual access is subject to a considerable number of exemptions, including information relating to national security, crime, taxation, health, education, social work, and parental records and reports.<sup>71</sup>

The Data Protection Principles of the 1998 Data Protection Act are very similar to the 1984 Act and require personal information to be: (1) fairly and lawfully processed; (2) processed for limited purposes; (3) adequate, relevant, and not excessive; (4) accurate; (5) not kept longer than necessary; (6) processed in accordance with individual rights; (7) kept secure; and, (8) not transferred without adequate protection.<sup>72</sup>

## 2. *The Human Rights Act*

The Data Protection Act was part of a broader recognition in United Kingdom law of a need to protect the right to privacy. The Data Protection Act was accompanied in the same year by another act, the Human Rights Act, which provided yet another drastic change in the protection of privacy rights.<sup>73</sup>

The Human Rights Act, by far the greatest protection of privacy rights the United Kingdom has ever codified, incorporated the European Convention on Human Rights into domestic law.<sup>74</sup> By adopting the European Convention on Human Rights, an international agreement that includes a specific right to

---

<sup>64</sup> *Id.* § 13.

<sup>65</sup> *Id.* § 7(1)(b)(i).

<sup>66</sup> *Id.* § 10.

<sup>67</sup> *Id.* § 11.

<sup>68</sup> *Id.* § 12.

<sup>69</sup> *Id.* § 14(1).

<sup>70</sup> *Id.* § 12A(1)(a).

<sup>71</sup> *Id.* §§ 28–30.

<sup>72</sup> *Id.* sched. 1, pt. I.

<sup>73</sup> Human Rights Act, 1998, c. 42 (Eng.).

<sup>74</sup> *Id.*

privacy,<sup>75</sup> Parliament effectively established, for the first time in Great Britain, an enforceable right to privacy.<sup>76</sup> Passage of the Human Rights Act further demonstrates a desire by British subjects, and their representatives in Parliament, to protect the individual right to privacy.

### C. Public Opinion

#### 1. Public Support for the Identity Cards Act

Supporters of the Identity Cards Act, including then Prime Minister Tony Blair and Home Secretary David Blunkett, often cite public support as a justification for the NIDS scheme.<sup>77</sup> Indeed, historical security measures undertaken by the British government tend to suggest that the British value security over privacy.<sup>78</sup> For example, Great Britain has made use of public closed circuit television surveillance since 1985.<sup>79</sup> According to Privacy International, a London-based campaign group, and the United States Electronic Privacy Information Center, Great Britain's security measures since September 11, 2001 demonstrate a far greater erosion of individual privacy rights than in any other developed country.<sup>80</sup> As the argument goes, since such drastic measures have been passed with little or no public resistance, it stands to reason that Britains are more concerned with national security than with personal privacy, and therefore more likely to approve of national identification cards. Indeed, early opinion polls reflected this prediction and

---

<sup>75</sup> ECHR, *supra* note 27, art. 8.

<sup>76</sup> Human Rights Act, Long Title.

<sup>77</sup> Michael Holden, *British Lawmakers Criticise Plans for ID Cards*, REUTERS NEWS, July 29, 2004.

<sup>78</sup> SURVEILLANCE, CLOSED CIRCUIT TELEVISION AND SOCIAL CONTROL, *supra* note 25.

<sup>79</sup> *Id.* at 9 (“[A]s the rise of [Closed Circuit Television] Surveillance easily evokes Orwellian concerns of Big Brother, we may ask why there has been so little public resistance or challenge.”). In addition, some criminal and other public laws have been passed in recent years with significant implications for the right to privacy. See Banisar & Davies, *supra* note 23, at 106.

<sup>80</sup> David Rowan, *Britain ‘Leads Way’ in Eroding Privacy*, TIMES (London), Sept. 5, 2002, at 16 (“Individual privacy is being eroded in Britain at a far greater pace than in other developed countries, according to an international study of state surveillance in the year since September 11 . . . . In the 400-page report, . . . Privacy International, a London-based campaign group, and the US Electronic Privacy Information Center, give warning of a significant loss of personal freedom. The Privacy and Human Rights survey notes that in many of the 53 countries studied, communications surveillance has grown, intrusive ‘personal profiling’ of individuals has increased, and data protection laws have been watered down.”).

showed strong public support for the scheme.<sup>81</sup> However, public support has dwindled over time,<sup>82</sup> consistent with Great Britain's historical uneasiness with national identification cards.

## 2. Public Response to Previous National Identification Schemes in the United Kingdom

The struggle over whether to implement a NIDS is not new to the United Kingdom.<sup>83</sup> Identity cards have been used during wartime, largely as a temporary measure to combat threats to national security.<sup>84</sup> The first use of national identity cards was during World War I, but they were abandoned in 1919.<sup>85</sup> Identity cards resurfaced during World War II under the National Registration Act of 1939, but were met with public disagreement.<sup>86</sup> The cards were officially abandoned in 1952 with the case *Willcock v. Muckle*, in which the judge said the cards were an "annoyance" and "tend[ed] to turn law-abiding subjects into law breakers."<sup>87</sup> Constrained by the technology of the

<sup>81</sup> Martin Hickman, *ID Cards Won't Cut Crime, UK Pressure Groups Say*, REUTERS NEWS, Sept. 24, 2001 (explaining that a *News of the World* newspaper poll reveals 85% of those polled support the identity cards use); *Blunkett Says Wants UK ID Cards in Three Years*, REUTERS NEWS, Apr. 25, 2004 (stating there is 80% popular support for identity card use according to MORI poll).

<sup>82</sup> Natalie Harrison, *Poll-Blair Seen Moving over for Brown as Early as 2006*, REUTERS NEWS, May 13, 2005 ("They [supporters of I.D. Cards] have this very reduced majority, there is a large part of the Labour party that [doesn't] support them . . . , the Liberal Democrats are completely against them. And I think the Conservatives are sceptical."); *ID Cards "Not a Panacea" for Terrorism – UK Minister*, REUTERS NEWS, Aug. 4, 2005 ("[R]ecent polls show public support for the scheme is falling.").

<sup>83</sup> See *History of ID Cards in the United Kingdom*, PRIVACY INT'L, Jan. 1, 1997, available at [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-61886&als\[theme\]=National%20ID%20Cards](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61886&als[theme]=National%20ID%20Cards).

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*; Press Release, Univ. of Cambridge, Identity Cards in Britain (Nov. 17, 2005), available at <http://www.admin.cam.ac.uk/news/press/dpp/2005111701>.

<sup>86</sup> *History of ID Cards in the United Kingdom*, *supra* note 83.

<sup>87</sup> *Willcock v. Muckle*, (1951) 2 K.B. 844, 851 ("[I]t is obvious that the police now, as a matter of routine, demand the production of national registration identity cards whenever they stop or interrogate a motorist for whatever cause. Of course, if they are looking for a stolen car or have reason to believe that a particular motorist is engaged in committing a crime, that is one thing, but to demand a national registration identity card from all and sundry, for instance, from a lady who may leave her car outside a shop longer than she should, or some trivial matter of that sort, is wholly unreasonable. This Act was passed for security purposes, and not for the purposes for which, apparently, it is now sought to be used. To use Acts of Parliament, passed for

time, both NIDS were paper based and did not involve recording information through a central database.<sup>88</sup> Over the years, failed attempts have been made to re-establish the card by the tax administration, immigration services, and the issuers of driver's licenses.<sup>89</sup> The latest attempt to introduce a NIDS, in 1995, was met by particularly strong criticism, including Tony Blair who demanded that, "instead of wasting hundreds of millions of pounds on compulsory ID cards . . . the money [should] provide thousands more police officers on the beat in our local communities."<sup>90</sup>

### 3. *Three Objections to the Identity Cards Act*

Although the 2006 Identity Cards Bill essentially met with strong public support, due to a concern for threats to national security and the need to improve verification systems and prevent fraud, public support for the scheme has melted away.<sup>91</sup> British subjects have grown uneasy about the national identification scheme for three basic reasons. First, people have begun to realize exactly how much identification cards would cost them.<sup>92</sup> In October 2006, the British government announced that the entire scheme would cost an estimated 5.4 billion pounds (\$10.08 billion) over the next ten years.<sup>93</sup>

Second, and relatedly, is the concern that the NIDS will fail to effectively meet its objectives.<sup>94</sup> Although the cards will make use of biometric data, making forgery more difficult for terrorists and other threats to national

---

particular purposes during war, in times when the war is past, except that technically a state of war exists, tends to turn law-abiding subjects into lawbreakers, which is a most undesirable state of affairs. Further, in this country we have always prided ourselves on the good feeling that exists between the police and the public and such action tends to make the people resentful of the acts of the police and inclines them to obstruct the police instead of to assist them." *Id.* at 851-52.

<sup>88</sup> Davies, *supra* note 1.

<sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> Hickman, *supra* note 81; *Blunkett Says Wants UK ID cards in Three Years*, *supra* note 81; Harrison, *supra* note 82; *ID Cards "Not a Panacea" for Terrorism - UK Minister*, *supra* note 82.

<sup>92</sup> Michael Holden, *Britain's ID Card Plan to Cost Billions of Pounds*, REUTERS NEWS, Oct. 9, 2006.

<sup>93</sup> *Id.*

<sup>94</sup> Philip Johnston, *Identity Cards Still Won't Work Home Front*, DAILY TELEGRAPH (U.K.), Dec. 6, 2004, at 19 (noting that "[d]etermined terrorists, . . . will not be prevented from carrying out their activities"). See also *Britain-Clarke Admits Identity Cards Will Not Prevent Future Terrorist Bombings*, MORNING STAR (U.K.), July 9, 2005.

security,<sup>95</sup> critics fear that most professionals will still be able to obtain fake identification cards.<sup>96</sup> Thus, according to critics, the benefits of the card do not justify the millions of pounds to be spent on compulsory identification cards.<sup>97</sup>

The third reason for dwindling public support of Britain's Identity Cards Act, and the most important for purposes of this Note, is the effect such a scheme will have on individual privacy rights.<sup>98</sup> A number of watch groups, including the Electronic Privacy Information Center and Privacy International, have taken a strong stance against the Identity Cards Act because of concerns with individual privacy.<sup>99</sup> Many British subjects share the same concerns.<sup>100</sup> Given the extensive amount of information collected on the national database under the plan, critics fear the Identity Cards Act is yet another step in the direction of "Big Brother" surveillance and fear the watchful eye of a totalitarian government.<sup>101</sup>

#### 4. *The Response of Other Governmental Entities*

As public support for the Identity Cards Act dwindled, so did that of Parliament and other government agencies.<sup>102</sup> Information Commissioner Richard Thomas has publicly attacked the scheme because of the extensive scope of the information to be recorded, and its possible implications for data protection laws.<sup>103</sup> Even the House of Lords/House of Commons Joint

<sup>95</sup> Matar, *supra* note 10, at 315.

<sup>96</sup> See Johnston, *supra* note 94; *Britain-Clarke Admits Identity Cards Will Not Prevent Future Terrorist Bombings*, *supra* note 94.

<sup>97</sup> Holden, *supra* note 92 ("The Cards . . . have drawn much criticism, . . . with opponents saying they will be . . . a costly flop.").

<sup>98</sup> *UK's Blair Wins Key Vote on Identity Cards*, REUTERS NEWS, Dec. 20, 2004 ("[C]ritics say [ID cards] pose a dangerous threat to civil liberties.").

<sup>99</sup> See *National ID Cards and REAL ID Act*, *supra* note 1; Davies, *supra* note 1.

<sup>100</sup> *U.K.'s Blair Wins Key Vote on Identity Cards*, *supra* note 98.

<sup>101</sup> *Id.*

<sup>102</sup> See, e.g., Patrick Wintour, *ID Cards Will 'Reveal Details of Daily Life'*, GUARDIAN (U.K.), June 28, 2005 (the Identity Cards Act has been criticized by the Information Commissioner); HOUSE OF LORDS-HOUSE OF COMMONS JOINT COMMITTEE ON HUMAN RIGHTS, *IDENTITY CARDS BILL, 2004-5*, H.C. 283.

<sup>103</sup> INFO COMM'RS OFF., *THE IDENTITY CARDS BILL-THE INFORMATION COMMISSIONERS CONCERNS* (Oct. 2005) ("The Information Commissioner is concerned that the extensive personal information retained on the proposed National Identity Register and the requirement on individuals to keep notifying changes is excessive and disproportionate. . . . The system of operation envisaged by the Government raises additional serious concerns."), available at [http://www.ico.gov.uk/upload/documents/library/corporate/detailed\\_specialist\\_guides/id\\_cards\\_bill\\_](http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/id_cards_bill_)



Committee on Human Rights, which examines every bill presented to Parliament, expressed deep concerns that the proposed Bill violated a notion of individual privacy.<sup>104</sup>

Thus, public opinion on individual privacy in the United Kingdom is somewhat mixed, with little or no resistance historically to privacy-stripping security measures on the one hand, and a deep hesitation when it comes to national identity cards on the other. As public opinion polls and government reports show, many British subjects and government officials are wary of the Identity Cards Act.

### III. THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND ITS PROTECTION OF THE RIGHT TO PRIVACY

#### A. *The Convention*

The European Convention on Human Rights, which has been incorporated by Parliament into domestic United Kingdom Law,<sup>105</sup> includes within its various protections a specific enforceable right to privacy.<sup>106</sup> That right, enshrined in Article 8 of the Convention, reads as follows:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.<sup>107</sup>

---

[\\_ico\\_concerns\\_october\\_2005.pdf](#)

<sup>104</sup> HOUSE OF LORDS, *supra* note 102.

<sup>105</sup> Human Rights Act, 1998, c. 29 (Eng.).

<sup>106</sup> ECHR, *supra* note 27, art. 8.

<sup>107</sup> *Id.*

*B. Article 8 Interferences (Triggers)*

In interpreting Article 8 of the Convention, the European Court of Human Rights has interpreted "private life," a respected right which all people should enjoy, to include activity that occurs within the home and to which people have a reasonable expectation of privacy,<sup>108</sup> as well as personal information which people consider private.<sup>109</sup>

With regard to personal information, the European Court of Human Rights has specifically held that the gathering and recording of personal data by government agencies alone triggers rights under Article 8 of the Convention.<sup>110</sup> According to the court, the use and disclosure of such information implicates Article 8 rights as well.<sup>111</sup> The court has construed information relating to private life very broadly,<sup>112</sup> and has held that the collection of even publicly available information, which may include a person's name, residence and other identifying characteristics, implicates the right to privacy, when the information is "systematically collected and stored."<sup>113</sup> In addition, the court applies a somewhat heightened standard of review when there has been an infringement of the right to privacy that involves particularly personal data such as medical records.<sup>114</sup>

---

<sup>108</sup> See, e.g., *Elahi v. United Kingdom*, 44 Eur. Ct. H.R. 30, ¶ 20 (2007) (explaining covert listening device placed in citizen's home implicates Article 8 right to respect for private life concerns).

<sup>109</sup> See, e.g., *Segerstedt-Wiberg v. Sweden*, 44 Eur. Ct. H.R. 2, ¶ 72 (2007) (storage of secret information about citizens by the police interferes with Article 8 rights); *R (on the application of S) v. Chief Constable of South Yorkshire*, [2002] EWCA (Civ) 1275 (Eng.) (holding collecting and maintaining fingerprints and DNA samples of individuals who have not been criminally convicted interferes with the right to private life).

<sup>110</sup> *R (on the Application of S)*, [2002] EWCA (Civ.) 1275 (recording of personal data including fingerprints constitutes an interference with Article 8 rights).

<sup>111</sup> *Leander v. Sweden*, 9 Eur. Ct. H.R. 433 (1987).

<sup>112</sup> *Niemietz v. Germany*, 16 Eur. Ct. H.R. 97 (1993) ("The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life.' However, it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world.")

<sup>113</sup> *Rotaru v. Romania*, 8 B.H.R.C. 43, ¶ 43 (2000) ("[P]ublic information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past.")

<sup>114</sup> *Z v. Findland*, 25 Eur. Ct. H.R. 371 (1997) ("[T]he protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life.")

On the other hand, the European Court of Human Rights has addressed the issue of national identification cards in the past.<sup>115</sup> According to the court, the issue of an identity card containing only a person's name, sex, date and place of birth, current address, and the name of their spouse does not in itself concern the right to private life under Article 8.<sup>116</sup> Furthermore, the obligation to hold or carry such a card is an insufficient intrusion to trigger Article 8 analysis.<sup>117</sup>

Once a possible infringement of Article 8 rights has been identified, the European Court of Human Rights undertakes analysis under Article 8.2 to determine if such interference is justified.<sup>118</sup> This analysis contains three steps: (1) whether the interference is in accordance with the law; (2) whether the interference serves one of the legitimate aims specifically listed in Article 8.2; and (3) whether the interference is necessary and proportionate to the aim it seeks to serve.<sup>119</sup>

### C. "In Accordance with the Law"

First, the European Court of Human Rights will find a violation of Article 8 where the interference with the privacy right is not in accordance with the law.<sup>120</sup> This analysis actually contains two steps. First, the court looks to domestic law to determine whether a particular interference is authorized.<sup>121</sup> Simply put, the Court looks for a statute or common law principle that specifically authorizes the challenged activity.<sup>122</sup> If no such authorization can be found—or worse, there is a specific law or regulation forbidding the activity<sup>123</sup>—the interference will be held a violation of Article 8.<sup>124</sup> Moreover,

<sup>115</sup> *Reyntjens v. Belgium*, 73 D.R. 136, 152 (1992).

<sup>116</sup> *Id.*

<sup>117</sup> *Id.*

<sup>118</sup> To see how the European Court of Human Rights has interpreted Article 8.2, see *Leander v. Sweden*, 9 Eur. H.R. Rep. 433, ¶ 48 (1987).

<sup>119</sup> *Leander*, 9 Eur. H.R. Rep. 433.

<sup>120</sup> *Id.*

<sup>121</sup> See *Elahi v. United Kingdom*, 44 Eur. Ct. H.R. 30, ¶ 20 (2007) (explaining use of covert listening devices not in accordance with the law because there exists no legally binding publicly accessible body of law regulating such activity); *Pisk-Piskowski v. Poland*, Eur. Ct. H.R. 92/03, ¶ 28 (2005) (stating censorship of convict's letters not in accordance with the law because Polish law provides a clear prohibition against such censorship).

<sup>122</sup> See *Elahi*, 44 Eur. Ct. H.R. 30, ¶ 20.

<sup>123</sup> See *Pisk-Piskowski*, Eur. Ct. H.R. 92/03, ¶ 28.

<sup>124</sup> *Elahi*, 44 Eur. Ct. H.R. 30, ¶ 20.

where there is statutory or other authorization for the conduct, the Court of Human Rights will also undertake analysis of the nation's Constitution or other charter document to determine if the authorization is compatible.<sup>125</sup>

In contrast, the second line of inquiry under "in accordance with the law" jurisprudence can invalidate challenged interferences regardless of whether they are authorized by statute.<sup>126</sup> According to the court, "in accordance with the law" not only requires the impugned measure have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and be compatible with the rule of law.<sup>127</sup> Further, the court explains "that a rule is 'foreseeable' if it is formulated with sufficient precision to enable any individual — with appropriate advice if need be — to regulate his conduct."<sup>128</sup> Thus, the court held that interference with the correspondence of death row inmates was not sufficiently foreseeable under a statute authorizing regulation of correspondence of those sentenced to imprisonment.<sup>129</sup> With regard to interferences that may be conducted in secret, such as undercover surveillance or wiretaps, foreseeability is arguably not possible because the persons whose rights are being interfered with may be unaware of the activity. However, the court places specialized restrictions on government actors in such situations.<sup>130</sup> Because secret surveillance is not open to scrutiny by the individuals whose interests are being invaded, legal discretion to conduct such surveillance may not be expressed in terms of

---

<sup>125</sup> See, e.g., *Segerstedt-Wiberg v. Sweden*, 44 Eur. Ct. H.R. 2, ¶ 42 (2006).

<sup>126</sup> See, e.g., *Dankevich v. Ukraine*, 38 Eur. Ct. H.R. 25, ¶ 157 (2003) (although restrictions on correspondence by incarcerated persons were specifically authorized by statute, it was not foreseeable that the measure applied to persons awaiting execution).

<sup>127</sup> *Segerstedt-Wiberg*, 44 Eur. Ct. H.R. 2, ¶ 42; *Leander v. Sweden*, 9 Eur. H.R. Rep. 433, 450, ¶ 51 (1987) ("[T]he requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. . . . Nevertheless, . . . the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life.").

<sup>128</sup> *Rotaru v. Romania*, 8 B.H.R.C. 43, ¶ 55 (2000).

<sup>129</sup> *Dankevich*, 38 Eur. Ct. H.R. 25, ¶ 156 ("The Court considers that it is not clear that persons sentenced to death are included among persons sentenced to imprisonment within the meaning of the Code, a death sentence being imposed because the offender is deemed incapable of reform through imprisonment.").

<sup>130</sup> See *Rotaru*, 8 B.H.R.C. 43, ¶ 55.

“unfettered power.”<sup>131</sup> Rather, the law must clarify the scope of the power to conduct such surveillance in order to protect against arbitrary interference.<sup>132</sup>

#### *D. Legitimate Aims*

Once satisfied that a measure is in accordance with the law, The European Court of Human Rights next inquires into whether the interference with the privacy right serves one of the legitimate aims listed in Article 8.2.<sup>133</sup> According to Article 8.2, a measure that interferes with the right to privacy is only justified if it advances one of the following interests: (1) national security; (2) public safety or the economic well-being of the country; (3) prevention of disorder or crime; or, (4) protection of the rights and freedoms of others.<sup>134</sup> The court is traditionally deferential to lawmakers and policymakers’ justifications for such measures, placing little scrutiny on the given statutory aims.<sup>135</sup> Thus, the collection of DNA and fingerprint samples was held to be for the legitimate purpose of prosecuting and preventing crime.<sup>136</sup> Also, forbidding a husband in jail from corresponding with his wife, who was suspected of being involved in the alleged crime for which he was being detained, was justified by the aims of securing the conduct of criminal proceedings and eliminating the risk of collusion, and was held to fall within the scope of prevention of disorder or crime, although the measure was invalidated for other reasons.<sup>137</sup>

#### *E. “Necessary in a Democratic Society”*

Finally, although a particular measure may satisfy the court as serving a legitimate aim, the measure may nevertheless be invalidated if it is not “necessary in a democratic society.”<sup>138</sup> The court has interpreted this to mean

---

<sup>131</sup> *Id.*

<sup>132</sup> *Id.*

<sup>133</sup> *Leander v. Sweden*, 9 Eur. H.R. Rep. 433, ¶ 48(1987).

<sup>134</sup> ECHR, *supra* note 27, art. 8.2.

<sup>135</sup> *See, e.g., Klamecki v. Poland* (No. 2), 38 Eur. Ct. H.R. 7, ¶ 147 (2003); *R (on the application of S) v. Chief Constable of South Yorkshire*, [2002] EWCA (Civ.) 1275, ¶ 34 (2002) (Eng.).

<sup>136</sup> *R (on the application of S)*, [2002] EWCA (Civ.) 1275, ¶ 39.

<sup>137</sup> *Klamecki*, 38 Eur. Ct. H.R. 7, ¶ 47 (explaining that although this case involved the right to respect for correspondence, another Article 8 right, the analysis is the same as if the measure implicated the right to respect for private life).

<sup>138</sup> ECHR, *supra* note 27, art. 8.2.

that the interference must be proportionate to the legitimate aim, with invasion of privacy rights to the minimum degree necessary to further the goal.<sup>139</sup> In other words, it must be shown that the aim could not be achieved by less intrusive means.<sup>140</sup> Thus, the court held that the collection of fingerprint and DNA samples for the purpose of prosecuting and preventing crime had no adverse consequences to the individual disproportionate to the public benefit.<sup>141</sup> On the other hand, refusing to allow a jail inmate to correspond with his wife, albeit for the proper purpose of preventing collusion, was held to be a disproportionate interference with the right to respect for correspondence.<sup>142</sup> Given the extreme intrusion, the court admonished the authorities for not considering alternative means.<sup>143</sup>

#### IV. GREAT BRITAIN'S NATIONAL IDENTIFICATION SCHEME: THE IDENTITY CARDS ACT 2006

##### *A. Background*

Britain's Identity Cards Act 2006 has been long in the making. Although not introduced to the public until after the terrorist attacks of September 11, 2001, a NIDS for the United Kingdom had been under way since 1999, when the Home Office began creating a prototype.<sup>144</sup> In 2003, Home Secretary David Blunkett first announced the proposal to introduce a British NIDS linked to a national identity database, the National Identity Register.<sup>145</sup> The scheme has been strongly advocated by Prime Minister Tony Blair, who claims the scheme is essential in the fight against terrorism, organized crime, and illegal immigration.<sup>146</sup>

The British Identity Cards Act met with strong resistance in Parliament, particularly from the Liberal Democrats and a large part of the Labour party,<sup>147</sup>

<sup>139</sup> *Leander v. Sweden*, 9 Eur. H.R. Rep. 433, ¶ 58 (1987) ("The notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.").

<sup>140</sup> *Id.*

<sup>141</sup> *R (on the application of S)*, [2002] EWCA (Civ.) 1275, ¶ 42.

<sup>142</sup> *Klamecki*, 38 Eur. Ct. H.R. 7, ¶ 152 (2003).

<sup>143</sup> *Id.*

<sup>144</sup> *Melissa Kite, National ID Card Ready After Secret Trial*, TIMES (U.K.), Nov. 1, 2001, at 2.

<sup>145</sup> *Davies*, *supra* note 1.

<sup>146</sup> *Britain's Ambitious ID Card Plan Comes Under Attack*, *supra* note 6.

<sup>147</sup> *Harrison*, *supra* note 82.

but was finally passed and entered the statute book on March 30, 2006 as the Identity Cards Act 2006.<sup>148</sup>

*B. The National Identity Register and “Registrable Facts”*

The Act creates a National Identity Register to be maintained by the Home Office, and to include certain information on each registered British subject.<sup>149</sup> The purposes of the Act include maintaining secure and reliable records, providing a convenient way for individuals to prove facts to others who require such proof, and providing a secure and reliable way to verify such facts whenever it is necessary in the public interest.<sup>150</sup> Thus, information may not be recorded, used or disclosed unless it is necessary in the public interest, which includes the following purposes: (1) “in the interests of national security”; (2) “for the purposes of the prevention or detection of crime”; (3) “for the purposes of the enforcement of immigration controls”; (4) “for the purposes of the enforcement of prohibitions on unauthorised working or employment”; and (5) “for the purpose of securing the efficient and effective provision of public services.”<sup>151</sup>

The “registrable fact[s]” eligible for recording on the Register include basic identity information, current and previous addresses, current residential status, all previous residential statuses, identification numbers, and “information about occasions on which the information recorded about [an individual] in the Register has been provided to any person.”<sup>152</sup> Included within the category of basic identity information are full name, gender, date and place of birth, date of death, and any external characteristics capable of identification.<sup>153</sup> In addition, the database will also contain biometric information such as fingerprints and iris scans.<sup>154</sup> All of this information may be maintained on the Register for as long as is consistent with the statutory purposes.<sup>155</sup>

---

<sup>148</sup> Davies, *supra* note 1.

<sup>149</sup> Identity Cards Act, 2006, c. 15, § 1(1) (Eng.).

<sup>150</sup> *Id.* § 1(3).

<sup>151</sup> *Id.* § 1(4).

<sup>152</sup> *Id.* § 1(5).

<sup>153</sup> *Id.* § 1(7).

<sup>154</sup> *Id.* §§ 5(4), 5(5), 7(3), 7(4) (indicating that once an individual becomes eligible and required to enter on the Register, he must allow his fingerprints and other biometric information about himself to be taken and recorded).

<sup>155</sup> *Id.* § 3(1)(b).

### C. *Entry on the Register*

There are three methods whereby information may be recorded on the Register. First, entitled individuals may apply to be entered on the Register.<sup>156</sup> Second, information from other sources capable of being recorded on the Register can be automatically recorded.<sup>157</sup> Third, information about individuals may be recorded on the Register when they apply for designated documents such as passports or driver's licenses.<sup>158</sup>

### D. *Disclosure of Information Contained on the Register*

According to the Act, information contained on the Register can be disclosed to various government agencies such as the Secret Intelligence Service and local law enforcement.<sup>159</sup> Also, the Act stipulates that regulations may make provision of public services conditioned on producing one's identification card.<sup>160</sup> Furthermore, the Act gives the Secretary of State power to extend the scope of eligible persons to whom information contained on the Register may be disclosed.<sup>161</sup>

### E. *Phasing In*

Because the NIDS will ultimately take several years to fully come into effect, identification cards will initially be introduced on a voluntary basis.<sup>162</sup> Beginning in 2008, all applications for new passports will require the collection of registrable data, including biometric information, and the issuance of an identification card.<sup>163</sup> Stand alone identification cards will eventually become compulsory for all British subjects over the age of sixteen.<sup>164</sup> The Act makes it clear, however, that British subjects will not be

---

<sup>156</sup> *Id.* § 2(1).

<sup>157</sup> *Id.* § 2(4).

<sup>158</sup> *Id.* § 4.

<sup>159</sup> *Id.* §§ 17(2)(b), 17(3).

<sup>160</sup> *Id.* § 13(1).

<sup>161</sup> *Id.* § 20(2).

<sup>162</sup> How the National Identity Scheme Will Get Started, *supra* note 8.

<sup>163</sup> *Id.*

<sup>164</sup> *Id.*



required to carry their identification cards and will not be asked to present them to officials.<sup>165</sup>

#### *F. Benefits*

According to the Identity and Passport Service, the NIDS entails numerous and wide ranging benefits, both for society as a whole and for the individual.<sup>166</sup> Among these benefits, the NIDS is expected to help protect cardholders against identity theft and fraud, provide a secure way of making financial transactions, and help to confirm eligibility for public services.<sup>167</sup> The benefits to society include helping to prevent organized crime and terrorism, combating illegal working, reducing illegal immigration into the United Kingdom, and allowing police to more quickly identify suspects and people they arrest.<sup>168</sup>

Despite apparent confidence in these benefits, the British government has publicly admitted overselling the advantages of the system.<sup>169</sup> Tony McNulty, the Home Office Minister in charge of the project at the time, admitted that previous suggestions that the cards “may well be a panacea for identity fraud, benefit fraud, terrorism, and entitlement and access to public services,” was a bit hasty, and that the government had wrongfully inflated the benefits of the plan in its enthusiasm to promote the scheme.<sup>170</sup>

### V. ANALYSIS UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS

#### *A. Article 8 Interference*

Great Britain’s Identity Cards Act raises serious concerns under the European Convention on Human Rights. First, the Act’s interference with the right to privacy is likely sufficient to warrant consideration under Article 8 of

---

<sup>165</sup> Identity Cards Act, § 16.

<sup>166</sup> Home Office, What are the Benefits of the National Identity Scheme?: Benefits at a Glance, <http://www.ips.gov.uk/identity/benefits-glance.asp> (last visited Mar. 28, 2008).

<sup>167</sup> *Id.*; see also Home Office, Using the Scheme in Daily Life, <http://www.ips.gov.uk/identity/how-icard-daily.asp> (last visited Mar. 24, 2008) (envisioning the use of identity cards and the accompanying personal identification number, similar to a credit card PIN number, in such routine daily activities as proving one’s age to purchase alcohol, collecting a parcel, and transferring money).

<sup>168</sup> What are the Benefits Of the National Identity Scheme?, *supra* note 166.

<sup>169</sup> *ID Cards “Not a Panacea” for Terrorism – UK Minister*, *supra* note 82.

<sup>170</sup> *Id.*

the Convention. Although the mere issuance of an identification card does not engage Article 8,<sup>171</sup> the European Court of Human Rights has never addressed a NIDS quite like that envisioned by the Identity Cards Act. A NIDS previously accepted by that court involved the collection and storage of only a person's name, sex, date and place of birth, current address, and the name of their spouse,<sup>172</sup> whereas Britain's Identity Cards Act is much more intrusive.

The Identity Cards Act allows for the collection of various private facts on the Register.<sup>173</sup> When systematically collected and stored in one central place, the culmination of these private facts can be very intrusive into a person's private life. By far the most intrusive of these is "information about occasions on which information recorded about [an individual] has been provided to any person."<sup>174</sup> This can include information on when the entry has been accessed by various government officials as well as public service providers,<sup>175</sup> thus leading to a detailed account of an individual's private life. For example, information can be provided to local law enforcement agencies in the course of routine criminal investigations, and can conceivably be maintained on the Register whether or not the individual has ever been convicted or even charged with a crime.<sup>176</sup>

The European Court of Human Rights has held that the gathering of personal data, even publicly available information when it is systematically collected and stored, triggers scrutiny under Article 8 of the Convention.<sup>177</sup> Therefore, the significant amount of information to be contained on the Register is likely a sufficient privacy invasion for Article 8 analysis. Furthermore, because holding information about a person's distant past has been held to raise particular privacy concerns,<sup>178</sup> the statutory language that allows information to be kept on the Register for as long as it is consistent with statutory purposes<sup>179</sup> is likely to concern the court. This could conceivably be a person's entire life. In addition, because the court has held that the use or

---

<sup>171</sup> *Reyntjens v. Belgium*, 73 D.R. 136, 152 (1992).

<sup>172</sup> *Id.*

<sup>173</sup> Identity Cards Act, 2006, c. 15, § 1(5) (Eng.).

<sup>174</sup> *Id.* § 1(5)(i).

<sup>175</sup> *Id.* §§ 13, 17.

<sup>176</sup> *Id.* § 17(3).

<sup>177</sup> *Friedl v. Austria*, 21 Eur. H.R. Rep. 83, ¶ 52 (1995); *Rotaru v. Romania*, 8 B.H.R.C. 43, ¶ 44 (2000).

<sup>178</sup> *Rotaru*, 8 B.H.R.C. 43, ¶ 55.

<sup>179</sup> Identity Cards Act, 2006, c. 15, § 13(1)(b) (Eng.).

disclosure of information also triggers Article 8,<sup>180</sup> the use and disclosure of information contained on the Register will do the same.

*B. “In Accordance with the Law”*

Second, the Identity Cards Act is likely not in accordance with the law. Although the Act is itself a statutory authorization and thus actions taken pursuant to it will be lawful in that respect, the European Court of Human Rights requires more than mere compliance with domestic law.<sup>181</sup> Because the law must be sufficiently clear and foreseeable as to put individuals on notice of its application to them,<sup>182</sup> the Identity Cards Act is likely to fail this prong of the analysis. Because information can be both entered into the Register and disclosed to third persons without the individual’s consent or knowledge,<sup>183</sup> the individual may be unaware that his privacy rights are being infringed. Also, because the Secretary of State has the power to expand the scope of persons eligible to receive information contained on the Register,<sup>184</sup> the extent to which an individual’s privacy is invaded is also unclear. The European Court of Human Rights is especially cautious when covert surveillance such as this is involved, and requires adequate measures to protect against arbitrary interference.<sup>185</sup>

*C. Legitimate Aims*

The Identity Cards Act is likely to pass muster under the third inquiry in the Article 8 analysis. The European Court of Human Rights requires that all interferences with the privacy interest be justified by legitimate government interests as described in Article 8.2.<sup>186</sup> The Identity Cards Act lists five statutory purposes, all of which would likely satisfy the court. The statutory purposes “in the interests of national security”<sup>187</sup> and “regarding the prevention or detection of crime”<sup>188</sup> track closely the language of Article 8.2, which lists

---

<sup>180</sup> *Leander v. Sweden*, 9 Eur. H.R. Rep. 433, ¶ 48 (1987).

<sup>181</sup> *Segerstedt-Wiberg v. Sweden*, 44 Eur. Ct. H.R. 2 (2006).

<sup>182</sup> *Id.*

<sup>183</sup> Identity Cards Act, §§ 2(4), 17, 18.

<sup>184</sup> *Id.* § 20(2).

<sup>185</sup> *Rotaru v. Romania*, 8 B.H.R.C. 43, ¶ 55 (2000).

<sup>186</sup> ECHR, *supra* note 27, art. 8.2.

<sup>187</sup> Identity Cards Act, § 1(4)(a).

<sup>188</sup> *Id.* § 1(4)(b).

the goals of national security and crime prevention as legitimate aims.<sup>189</sup> “For the purposes of the enforcement of immigration controls”<sup>190</sup> would likely satisfy the court as being related to national security. The remaining justifications, “for the purposes of the enforcement of prohibitions on unauthorised working or employment”<sup>191</sup> and “for the purpose of securing the efficient and effective provision of public services”<sup>192</sup> are more difficult to justify, but the Court may conceivably accept these as furthering the goal of economic well-being.<sup>193</sup>

D. “Necessary in a Democratic Society”

Even if the court accepts the justifications for the Identity Cards Act as legitimate, the Act is still subject to scrutiny under the fourth and final prong of the analysis—whether the interference is “necessary in a democratic society,”<sup>194</sup> or in other words, necessary and proportionate.<sup>195</sup> For several reasons, the court is unlikely to hold the invasion of privacy envisioned by the Identity Cards Act as either necessary or proportionate to the attainment of the stated goals.

First, the Act demands collection of too broad a range of information. The British government has been unable to advance any important reasons for requiring individuals to record certain information on the Register, such as all previous residences and all prior residential statuses.<sup>196</sup> The range of information to be contained on the Register is not proportionate to the stated goals of national security and crime prevention. Second, it is difficult to justify a scheme whereby interference with Article 8 privacy rights depends on whether an individual needs a new or renewed passport.<sup>197</sup> Because the scheme will be phased in by first requiring all persons applying for designated documents to register, the interference with the privacy right is disproportionate to the goal. Third, the Act envisions a broad array of information to be disclosed to a wide range of persons and agencies, including

---

<sup>189</sup> ECHR, *supra* note 27, art. 8.2.

<sup>190</sup> Identity Cards Act, § 1(4)(c).

<sup>191</sup> *Id.* § 1(4)(d).

<sup>192</sup> *Id.* § 1(4)(e).

<sup>193</sup> ECHR, *supra* note 27, art. 8.2.

<sup>194</sup> *Id.*

<sup>195</sup> *Leander v. Sweden*, 9 Eur. H.R. Rep. 433, ¶ 48 (1987).

<sup>196</sup> Identity Cards Act, § 1(5)(c)(g).

<sup>197</sup> How the National Identity Scheme will Get Started, *supra* note 8.

local law enforcement and the providers of public service benefits.<sup>198</sup> Because some of the information provided will be irrelevant to the purposes of the agencies, the interference with the privacy rights greatly exceeds that necessary to accomplish the goals.

Finally, as some critics have pointed out, concerns over whether the NIDS will work to effectively reach the goals of national security and the prevention of crime<sup>199</sup> also raise questions of proportionality under Article 8. Critics charge that a NIDS in other European countries such as France, Spain and Italy have failed to stop terrorist attacks.<sup>200</sup> According to Lord Carlile, Britain's reviewer of terrorism legislation, identity cards would only have "limited value" and would not have prevented the London subway bombing in July.<sup>201</sup> According to a recent report by Privacy International, two-thirds of all terrorists in history have operated under their true identity.<sup>202</sup> Thus, identity cards would have little preventative effect.<sup>203</sup> Other terrorists use a wide range of techniques to forge identities, and would likely be able to penetrate the system anyway.<sup>204</sup> Given the marginal utility of a NIDS such as Britain's Identity Cards Act, the interference with the right to privacy is highly disproportionate to any benefits that may be realized.

## VI. CONCLUSION

The expansive NIDS envisioned by the United Kingdom's Identity Cards Act is a dangerous intrusion upon civil liberties in the name of national security. The scheme violates a notion of privacy that has grown within the United Kingdom, with the latest and largest protection coming less than a decade ago.<sup>205</sup> The proposed policy is also contrary to the principles laid out

---

<sup>198</sup> Identity Cards Act, §§ 13, 17.

<sup>199</sup> See, e.g., Johnston, *supra* note 94.

<sup>200</sup> Hickman, *supra* note 81.

<sup>201</sup> *Success of ID Cards Questioned by Govt Reviewer*, REUTERS NEWS, Jan. 29, 2006.

<sup>202</sup> PRIVACY INT'L, MISTAKEN IDENTITY; EXPLORING THE RELATIONSHIP BETWEEN NATIONAL IDENTITY CARDS & THE PREVENTION OF TERRORISM 2 (2004) (also noting that "[a]t a theoretical level, a national identity card as outlined by the UK government could only assist anti-terrorism efforts if it was used by a terrorist who was eligible and willing to register for one, if the person was using their true identity, and if intelligence data could be connected to that identity"), available at <http://www.privac yinternational.org/issues/idcard/UK/id-terrorism.pdf>.

<sup>203</sup> *Id.*

<sup>204</sup> *Id.*

<sup>205</sup> Data Protection Act, 1998, c. 29 (Eng.); Human Rights Act, 1998, c. 42 (Eng.).

by the European Convention on Human Rights<sup>206</sup>—rights that are considered so fundamental in the United Kingdom that they were incorporated into domestic law.<sup>207</sup>

The possible privacy implications posed by the United Kingdom's Identity Cards Act are breathtaking. It is not difficult to imagine the public response that would follow if the United States were to propose legislation such as the Identity Cards Act. Yet, this scenario may not be merely a hypothetical one, even with the America's strong legal culture of safeguarding individual privacy rights. As it has in most other countries, the possibility of a NIDS has been discussed in the United States extensively in the years since September 11.<sup>208</sup>

Any country faced with the decision of whether to implement a NIDS must take into account both the interests of national security and individual privacy rights. Opposition to a NIDS should in no means be taken to demean the important government interest in national security. Most reasonable people would agree that national security is one of the most important goals of any civilized society. However, this interest must be weighed against the interest of privacy. Privacy is generally considered to be such an important fundamental right that it has been recognized in almost every civilized country as well as in various international agreements, such as the European Convention on Human Rights.<sup>209</sup>

In a democratic society, the fundamental interests of privacy need not be sacrificed in the name of national security. Prior to September 11, 2001, British Prime Minister Tony Blair once voiced his objection to a NIDS, saying “[i]nstead of wasting hundreds of millions of pounds on compulsory ID cards . . . the money [should] provide thousands more police officers on the beat in our local communities.”<sup>210</sup> Although this statement was made before the age of global terrorism, the same principle can be applied today: let the money provide better airport security, tighter border control, and more stringent immigration laws. These are options that would be much less

---

<sup>206</sup> ECHR, *supra* note 27.

<sup>207</sup> See Human Rights Act, 1998.

<sup>208</sup> See, e.g., Serge Egelman & Lorrie Faith Cranor, *Federal Secrecy After September 11 and the Future of the Information Society: The Real ID Act: Fixing Identity Documents with Duct Tape*, 2 J.L. & POL'Y INFO. SOC'Y 149 (2006) (discussing the Real ID Act, federal legislation designed to reform the drivers' licensing systems of all states in order to make the process more secure as well as uniform across America, and its implications for privacy including the observation that the Act will create a de facto National ID card).

<sup>209</sup> See *Privacy & Human Rights 2003: Overview*, *supra* note 18 and accompanying text.

<sup>210</sup> Davies, *supra* note 1.

invasive to the individual right to privacy. It is true that none of these methods would be foolproof. In fact, most countries have implemented these measures in the years following September 11, and none of them can be said to be completely protected from terrorist attacks or other grave breaches of national security. However, the same could be said of a NIDS. Even taking into consideration the thoroughness and breadth of the United Kingdom's scheme, there is no such thing as a perfect NIDS. Given that, it is difficult to justify the additional privacy interference posed by a NIDS.

As the United Kingdom goes forward with its national ID cards, it is imperative that United States legislators and policymakers take advantage of the valuable insight such an experiment can have on this country's own debate. Only time will tell whether the United Kingdom's Identity Cards Act will prove successful at combating terrorism and achieving its other goals, or whether it will lead to abuses of power and grave breaches of the right to privacy far exceeding the scope of its original purpose.

